Amendments to the Claims

1. (currently amended) A method for operating a public-key encryption scheme which provides for [[of]] sending a digital message M between a sender and a recipient ~~in a public-key encryption scheme comprising the sender, the recipient and~~ with participation of an authorizer as specified by operations (a) through (f) defined below, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising one or more of operations (R), (Au), (S), wherein:

the operation (R) comprises the operations (a), (f);

the operation (Au) comprises the operations (c), (d);

the operation (S) comprises the operation (e);

wherein the operations (a) through (f) are as follows:

(a) generating a recipient public key/ recipient private key pair, [[;]] wherein the recipient private key is a secret of the recipient;

(b) generating a recipient encryption key;

(c) selecting a key generation secret that is a secret of the authorizer;

(d) generating a recipient decryption key using at least the key generation secret and the recipient encryption key, wherein a key formed from the recipient decryption key and a key formed from the recipient encryption key are a public key/ private key pair;

(e) encrypting the digital message using at least the recipient public key and the recipient encryption key to create an encrypted digital message; and

(f) decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.

2. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

3. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

4. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the recipient public key.

5. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key

6. (Original) The method of claim 1, wherein the recipient decryption key is generated by the authorizer according to a schedule known to the sender.

7. (Original) The method of claim 6, wherein the recipient encryption key is generated using at least information comprising the schedule.

8. (Original) The method of claim 1, wherein the recipient private key/ public key pair is generated using at least one system parameter issued by the authorizer.

9. (currently amended) The method of claim 1, wherein generating the recipient decryption key ~~is generated by a method comprising~~ comprises:

~~(a)~~ generating a first cyclic group $\mathbb{G}_1$ of elements and a second cyclic group $\mathbb{G}_2$ of elements;

~~(b)~~ selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;

~~(c)~~ selecting a generator P of the first cyclic group $\mathbb{G}_1$;

~~(d)~~ selecting a random key generation secret s_C associated with and known to authorizer;

~~(e)~~ generating a key generation parameter $Q = s_C P$;

~~(f)~~ selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;

~~(g)~~ selecting a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$;

~~(h)~~ generating an element $P_B = H_1(\text{Inf}_B)$, wherein Inf_B comprises a string of binary digits; and

~~(i)~~ generating a secret element $S = s_c P_B$ associated with the recipient, [[;]] wherein the secret element is the recipient decryption key.

10. (Original) The method of claim 9, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

11. (Original) The method of claim 9, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

12. (Original) The method of claim 9 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

13. (Original) The method of claim 9 wherein the function $\hat{e}$ is a bilinear, non-degenerate, and efficiently computable pairing.

14. (Original) The method of claim 9 wherein:

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$;

Q is an element of the second cyclic group $\mathbb{G}_2$;

element P_B is an element of the first cyclic group $\mathbb{G}_1$; and

the secret element S is an element of the first cyclic group $\mathbb{G}_1$.

15. (currently amended) The method of claim 9, wherein encrypting the digital message M ~~is encrypted by a method comprising~~ comprises:

generating the element $P'_B = H_{1'}(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein $H_{1'}$ is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret r; and

encrypting the digital message M to form a ciphertext C_1 [[;]] wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where ~~$g = \hat{e}(Q, P_B)\hat{e}(s_BP, P'_B)$~~ $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key.

16. (Original) The method of claim 1, wherein the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document.

17. (currently amended) The method of claim 9, wherein encrypting the digital message M ~~is encrypted by a method comprising~~ comprises:

generating the element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C, [[;]] wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H4(\sigma)}(M)]$, where ~~$g = \hat{e}(Q, P_B)\hat{e}(s_B P, P'_B)$~~

$g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$,

wherein PK_B is the recipient public key, wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a ~~secure~~ symmetric encryption scheme, and H4(σ) is the key used with E.

18. (currently amended) A method for operating a public-key encryption scheme which provides for [[of]] sending a digital message between a sender and a recipient ~~in a public-key encryption scheme comprising the sender, the recipient and~~ with participation of a plurality of authorizers as specified by operations (a) through (g) defined below, the plurality of authorizers including a root authorizer and n lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, the method comprising one or more of operations (R), (RAu), (Au), (S), wherein:

the operation (R) comprises the operations (a), (g);

the operation (RAu) comprises the operations (c), (d);

the operation (Au) comprises the operation (e);

the operation (S) comprises the operation (f);

wherein the operations (a) through (g) are as follows:

(a) generating a recipient public key/ private key pair for the recipient, [[;]] wherein the recipient private key is a secret of the recipient;

(b) generating a recipient encryption key using identity information of at least one of the recipient's ancestors;

(c) selecting a root key generation secret that is a secret of the root authorizer;

(d) generating a root key generation parameter based on the root key generation secret;

(e) generating a recipient decryption key such that the recipient decryption key is related to the recipient encryption key, the root key generation secret and the associated root key generation parameter;

(f) encrypting the digital message using the recipient public key and a recipient encryption key to create an encrypted digital message, wherein a key formed from the recipient decryption key and a key formed from the recipient encryption key are a public key/ private key pair; and

~~(h)~~ (g) decrypting the ~~encoded~~ encrypted digital message to recover the digital message using at least the recipient private key and the recipient decryption key.

19. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

20. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

21. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the recipient public key.

22. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

23. (Original) The method of claim 18, wherein the recipient decryption key is generated according to a schedule known to the sender.

24. (currently amended) The method of claim 18, wherein the recipient private key/ public key pair is generated using system parameters issued by one or more of the authorizers ~~authorizer~~.

25. (Original) The method of claim 18, wherein the recipient decryption key is related to the root key generation secret and the associated root key generation parameter.

26. (currently amended) The method of claim 18, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, the ~~method~~ the public-key encryption scheme further comprising:

selecting a lower-level key generation secret for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

generating a sender decryption key such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor ~~authorizer$_l$~~ authorizer$_l$; and

wherein the ~~ciphertext~~ encrypted digital message is decrypted using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

27-116. (cancelled)

117. (new) The method of claim 1 wherein the method comprises the operation (R) performed by the recipient.

118. (new) The method of claim 1 wherein the method comprises the operation (Au) performed by the authorizer.

119. (new) The method of claim 1 wherein the method comprises the operation (S) performed by the sender.

120. (new) The method of claim 1 wherein the method comprises the operation (R) performed by the recipient and the operation (Au) performed by the authorizer.

121. (new) The method of claim 1 wherein the method comprises the operation (Au) performed by the authorizer and the operation (S) performed by the sender.

122. (new) The method of claim 1 wherein the method comprises the operation (R) performed by the recipient and the operation (S) performed by the sender.

123. (new) The method of claim 1 wherein the method comprises the operation (R) performed by the recipient, the operation (Au) performed by the authorizer, and the operation (S) performed by the sender.

124. (new) The method of claim 1 wherein the operation (b) is performed by the authorizer and/or the recipient and/or the sender.

125. (new) The method of claim 2 wherein the method comprises the operation (b).

126. (new) The method of claim 3 wherein the method comprises the operation (b).

126. (new) The method of claim 4 wherein the method comprises the operation (b).

127. (new) The method of claim 5 wherein the method comprises the operation (b).

128. (new) The method of claim 6 wherein the method comprises the operation (Au) performed by the authorizer.

129. (new) The method of claim 7 wherein the method comprises the operation (b).

130. (new) The method of claim 9 wherein the method comprises the operation (Au) performed by the authorizer.

131. (new) The method of claim 10 wherein the method comprises the operation (Au) performed by the authorizer.

132. (new) The method of claim 11 wherein the method comprises the operation (Au) performed by the authorizer.

133. (new) The method of claim 12 wherein the method comprises the operation (Au) performed by the authorizer.

134. (new) The method of claim 13 wherein the method comprises the operation (Au) performed by the authorizer.

135. (new) The method of claim 14 wherein the method comprises the operation (Au) performed by the authorizer.

136. (new) The method of claim 15 wherein the method comprises the operation (S) performed by the sender.

137. (new) The method of claim 16 wherein the method comprises the operation (Au) performed by the authorizer.

138. (new) The method of claim 16 wherein the method comprises the operation (R) performed by the recipient.

139. (new) The method of claim 17 wherein the method comprises the operation (S) performed by the sender.

140. (new) The method of claim 18 wherein the method comprises the operation (R) performed by the recipient.

141. (new) The method of claim 18 wherein the method comprises the operation (RAu) performed by the root authorizer.

142. (new) The method of claim 18 wherein the method comprises the operation (Au) performed by one of the authorizers.

143. (new) The method of claim 18 wherein the method comprises the operation (S) performed by the sender.

144. (new) The method of claim 18 wherein the method comprises the operation (R) performed by the recipient and the operation (Au) performed by one of the authorizers.

145. (new) The method of claim 18 wherein the method comprises the operation (R) performed by the recipient and the operation (S) performed by the sender.

146. (new) The method of claim 18 wherein the method comprises the operation (Au) performed by one of the authorizers and the operation (S) performed by the sender.

147. (new) The method of claim 18 wherein the method comprises the operation (R) performed by the recipient, the operation (Au) performed by one of the authorizers, and the operation (S) performed by the sender.

148. (new) The method of claim 18 wherein the method comprises the operation (b).

149. (new) The method of claim 19 wherein the method comprises the operation (b).

150. (new) The method of claim 20 wherein the method comprises the operation (b).

151. (new) The method of claim 21 wherein the method comprises the operation (b).

152. (new) The method of claim 22 wherein the method comprises the operation (b).

153. (new) The method of claim 23 wherein the method comprises the operation (Au) performed by one of the authorizers.

154. (new) The method of claim 25 wherein the method comprises the operation (Au) performed by one of the authorizers.

156. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 1.

157. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 5.

158. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 9.

159. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 10.

160. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 11.

161. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 13.

162. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 15.

163. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 16.

164. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 17.

165. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 18.

166. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 20.

167. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 22.

168. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 23.

169. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 26.

170. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 117.

171. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 118.

172. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 119.

173. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 123.

174. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 127.

175. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 130.

176. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 136.

177. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 140.

178. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 141.

179. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 142.

180. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 143.

181. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 147.

182. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 150.

183. (new) A manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 152.